Universität Basel Max Kehm max.kehm@stud.unibas.ch
Institut für Soziologie
Proseminar: Sicherheit und Versicherung. Machtanalysen im Anschluss an Michel Foucault

Das Neoliberale Panoptikum – Staatliche Sicherheit und Privatwirtschaftliche Infrastruktur

In den letzten den letzten Jahrzehnten war und ist die Diskussion um die Schaffung von mehr Sicherheit ein dominantes Thema im politischen Diskurs.
Bei den Verschärfungen der Inneren Sicherheit, welche quasi weltweit in allen Industriestaaten stattgefunden haben, handelt es sich meist um den Ausbau digitaler Überwachungstechnologien. Angefangen von der Vorratsdatenspeicherung, über Bundestrojaner bis hin zum Aufbau von weitreichenden Personenbezogenen Datenbanken wie z.B. der "No Fly List" der USA. Zudem findet eine immer engere Kooperation zwischen dem staatlichen Sicherheitsapparat und privaten Akteuren statt. Dies wird Beispielsweise bei der Vorratsdatenspeicherung ersichtlich bei welcher die Provider ihre Datenbanken und Server zur Speicherung der anfallenden Datenmenge zur Verfügung stellen sollen.

John Kannankulam (Kannankulam 2009: 3-4) führt den zunehmenden Ausbau der Sicherheitsappperate auf die Änderung der kapitalistischen Produktionsweise, den Wechsel vom Fordismus zum Postfordismus zurück. Der Fordismus war noch von der Gewährung einer gewissen sozialen Sicherheit, Vollbeschäftigung sowie einem funktionierenden Wohlfahrtsstaat geprägt, der auch im Falle von Krankheiten oder im Alter eine soziale Sicherungsfunktion übernahm. Das engere Netz der sozialen Sicherheit war jedoch auch ein Mechanismus der sozialen Kontrolle, sodass jene, die von der standardisierten Norm abwichen, leicht diszipliniert werden konnten. Diese engen Strukturen wurden jedoch mit der Durchsetzung des Neoliberalismus weitgehend aufgelöst, mit der Folge, dass nun der Wettbewerb der einzelnen Individuen untereinander im Vordergrund steht und die sozialen Sicherungsnetze zunehmend aufgelöst werden. Dies führt für das einzelne Individuum zwar tatsächlich zu mehr "Freiheit", die immer weitergehende Individualisierung des Einzelnen birgt jedoch auch für das System das Risiko, dass sich die Individuen verselbständigen und sich dem System entziehen (Kannankulam 4). Vor allem die steigenden Unsicherheiten auf dem Arbeitsmarkt sowie die zunehmende Arbeitslosigkeit sorgen laut Kannankulam dafür, dass immer mehr Individuen aus dem Verwertungsprozess ausgeschlossen werden und somit zu einem Risikofaktor werden, welchen es durch den Ausbau der staatlichen Sicherheitsmechanismen zu kontrollieren gilt. Also gerade jene neoliberalen und neokonservativen Kräfte, welche in Bezug auf den Markt den Staat zu ihrem eigenen Vorteil zurückzudrängen wollen, fordern den immer weitergehenden Aufbau der staatlichen Sicherheit, um die durch den Prozess der Neoliberalisierung benachtiligten Bevölkerungsschichten unter Kontrolle zu halten.
Diese Analyse wird nicht zuletzt durch die unkontrollierten Aufstände und Plünderungen in den Banlieus von Frankreich und England gestärkt, welche maßgeblich von den wirtschaftlich benachteiligten Bevölkerungsteilen mitgetragen wurden.

In diesem Essay möchte ich untersuchen inwieweit Kannankulams Theorie als Erklärung für den Offensichtlich immer weiteren Ausbau des Sicherheitsstaates anwendbar ist, bzw inwiefern man noch weitere Faktoren hinzuziehen muss, um diese Entwicklung erklären zu können. Meiner Ansicht nach sollte stärker mit einbezogen werden, dass die zunehmende Kontrolle und Überwachung letztendlich erst durch den rasanten technischen Fortschritt in der Computertechnik der letzten zwei Jahrzehnte möglich geworden ist. Infolge dieser Entwicklung wird es für Staat und privatwirtschaftliche Akteure immer einfacher, riesige Datenmengen zu speichern und auszuwerten. Vor allem privatwirtschaftliche Akteure scheinen dabei eine immer größere Rolle zu spielen wie die zunehmende Kooperation von Geheimdiensten mit Konzernen wie Facebook oder Google nahelegt. Daher werde ich im folgenden die zunehmende Vernetzung Staatlicher und Privatwirtschaftlicher Akteure in der Schaffung öffentlicher Sicherheit und deren Folgen näher analysieren.

Es greift meiner Meinung nach zu kurz, den steigenden Ausbau der Inneren Sicherheit primär auf die Änderung der Produktionsweise zurückzuführen. Schließlich wurden auch schon in der Blütezeit des Fordismus massiv autoritäre Strukturen geschaffen, um mögliche Risikogruppen in der Bevölkerung unter Kontrolle zu halten. Als Exempel kann hier die Mc Carthy Ära dienen, in welcher es in den USA zu massiver Überwachung und Repression gegen jene kam, denen man linke Umtriebe unterstellte. Dabei kam dem FBI die Aufgabe zu, unerwünschte Gruppen und Individuen zu überwachen und mit den Mitteln der Repression zu bekämpfen. Auch in den Diktaturen des ehemaligen Ostblocks wurden Trotz planwirtschaftlich organisierter Produktionsweise und somit enger Kontrolle der Menschen an ihrem Arbeitsplatz und anderen staatlich organisierten Gesellschaftsbereichen ein umfangreicher Überwachungsapparat geschaffen. Es scheint somit das staatlich organisierte Gesellschaften generel die Tendenz haben einen massiv in die Sicherheit zu investieren. Selbst tendenziell Basisdemokratisch organisierte Gesellschaften wie die Schweiz scheinen wie der Fichenskandal belegt nicht vor solchen Entwicklungen ausgenommen zu sein.

Es kann also nicht davon ausgegangen werden, dass der verstärkte Ausbau der staatlichen Sicherheit primär durch den Wechsel der Produktionsweise hin zum Postfordismus/Neoliberalismus zu erklären ist.
Der Übergang zur neoliberalen Wirtschaftsideologie kann jedoch eine Erklärung dafür sein, warum vermehrt privatwirtschaftliche Unternehmen in die Schaffung der öffentlichen Sicherheit mit einbezogen werden und somit ein lukrativer, staatlich finanzierter und durchgesetzer Markt für Sicherheitsprodukte entsteht. Angefangen von den Technologien der Biometrie bis hin zur Entwicklung intelligenter Kamerasysteme, welche über die Fähigkeit verfügen, Gesichter und Personen automatisiert zu erkennen und mit Internetbasierten Datenbanken abzugleichen. Besonders deutlich wird dies bei Firmen, die aus kommerziellen Interessen ohnehin schon umfangreiche Datenbanken betreiben, um detailierte Profile zu erstellen, die dann auch von der werbetreibenden Industrie genutzt werden können. Was liegt also näher, als die bereits vorhandenen privatwirtschaftlichen Datenbanken mit denen der staatlichen Sicherheit zu vernetzen. Namhafte Geheimdienste wie der CIA haben schon längst Abteilungen, die die enormen Datenmengen in den sozialen Netzen ansammeln, auswerten und analysieren. (Dozier 2011: Link)
Ein weiterer Faktor dürfte sein, dass ein Großteil der Technologieentwicklung privatwirtschaftlich durchgeführt wird und das Produkt davon, die Technologie, die Algorithmen das urheberrechtlich und patentiert geschützte Eigentum der entsprechenden Firmen sind. Der Staat ist also mehr und mehr darauf angewiesen, mit Privatanbietern zu kooperieren, um an die für den weiteren Aufbau des Sicherheitsregimes benötigte Technologie zu gelangen. So kooperieren zum Beispiel der CIA und Google bei der Entwicklung von neuen Technologien zur Analyse sehr großer Datenmengen mit dem Ziel, zukünftige politische und soziale Risiken frühzeitig erkennen zu können. (Simonite 2010: Link).

Es liegt auf der Hand, dass die weitreichenden Überwachungs- und Sicherheitsmaßnahmen, die derzeit diskutiert oder umgesetzt werden, nur möglich sind, weil die dafür benötigte Technologie zur Verfügung steht. Die Möglichkeiten, Daten zu speichern und tiefgehend zu analysieren, steigen mit der digitalen Revolution exponentiell an. War es früher noch nötig, riesige Aktenberge in Papierform vorrätig zu halten, Überwachungsaufnahmen mit Hilfe der Schreibmaschine aufwändig auf Papier zu tippen und so zu protokollieren, lassen sich heute solche Vorgänge weitgehend vollständig automatisieren. Moderne Spracherkennungssoftware ist in der Lage, Telefongespräche automatisch in Text zu verwandeln und in durchsuchbaren Datenbanken zu speichern oder, sofern eine bestimmte Kombination von Schlagwörtern fallen, automatisch die Sicherheitsbehörden zu informieren bzw die Kommunikationsverbindung zu kappen. Auf diese Weise funktioniert zum Beispiel das digitale Überwachungs- und Zensursystem in China.
Da Text nur sehr geringen Speicherplatz belegt, wäre es somit technisch gesehen leicht, sämtliche Telekommunikationsvorgänge eines ganzen Staates, die auf Sprache basieren, zu analysieren und

auf Jahre hinaus zu archivieren. Beim Emailverkehr ist diese Praxis auch in Deutschland längst üblich. So hat der BND im Jahr 2010 um die 37 Millionen E-Mails abgefangen und ausgewertet. (Der Spiegel 2012: Link).

Völlig neue Möglichkeiten erschließen sich jedoch durch die Entwicklung künstlicher Intelligenz. So entwickelt zum Beispiel der amerikanischer Militärkonzern Raytheon ein System, das automatisch alle verfügbaren Daten aus dem Internet analysiert und in einen passenden Kontext einordnet. So ist das System vollautomatisiert in der Lage, umfangreiche Dossiers zu Personen und Organisationen zu erstellen. Zwar enthalten die erstellten Texte noch immer Fehler und sind daher noch nicht voll einsatzfähig. jedoch ist absehbar, dass die Fähigkeiten der artifiziellen Textverarbeitung mit dem weiteren exponentiellen Ansteigen der Rechenkapazitäten zunehmen werden und Fehlfunktionen durch ausgefeiltere Algorithmen reduziert werden können. (Talbot 2012: Link)
Werden nun solche Technologien mit der Möglichkeit kombiniert, auf die Datenbanken von Google, Facebook, Walmart usw zuzugreifen, wäre es leicht, vollständig automatisiert Persönlichkeitsprofile der gesamten Bevölkerung zu erstellen. In wie weit dies bereits geschieht, ist nicht bekannt da, es eher selten vorkommt, dass die Aktivitäten der Geheimdienste einer breiten Öffentlichkeit bekannt werden.
Auch bei der regulären Polizei kommen in den USA vermehrt Systeme der künstlichen Intelligenz zum Einsatz, um mögliche Verbrechen vorhersagen zu können. Dabei werden geographische, statistische und zahlreiche persönliche Daten in die Berechnungen mit einbezogen. Die Zeit berichtet:

"*Als die Frau mit den Drogen durch die Tiefgarage im kalifornischen Santa Cruz lief und immer wieder Blicke in die geparkten Autos warf, wartete die Polizei schon auf sie. Die Beamten wussten, dass sie kommen würde. Sie hatten es berechnet. Genauer gesagt: Sie hatten berechnet, dass irgendjemand kommen würde, den sie würden festnehmen können.*"
(Beuth 2011: Link)

Letztendlich wird es so möglich, Gefährdungsprofile von einer immer größer werdenden Anzahl von Individuen quasi in der Cloud vorher zu berechnen, sodann entsprechende präventive Maßnahmen einlzueiten, um zu verhindern das aus einem potentiellen Risiko Realität wird.
So wird bereits ähnliche Software im Gefängnissbetrieb eingesetzt um die Wahrscheinlichkeit zu berechnen, mit welcher ein Häftling Gewalttaten begehen wird, wenn er auf Bewährung freigelassen würde. Der Algorithmus entscheidet somit maßgeblich über die Zukunft jener Menschen deren Risikopotential er berechnen soll. (Bland 2010: Link) Die Künstliche Intelligenz wird somit mehr und mehr zu einem mächtigen Herrschaftsmechanismus und das in doppelter Hinsicht: Zum einen indem sie über die Zukunft möglicher Risikoindiviudue entscheidet, zum anderen aber auch indem die Sicherheitsbehörden zunehmend den Empfhelungen der Maschine folgen und somit eigene Handlungsfreiheit aufgeben.
Bisher kommen solche Systeme noch primär in der Terror- und Kriminalitätsbekämpfung zum Einsatz. Wikileaks hat jedoch die Existenz des Überwachungssystems "Trapwire" aufgedeckt, an dem auch der Privatgeheimdienst Stratfor beteiligt war. Interne Mails legen nahe das Trapwire u.a für die Analyse der Bedrohung durch "Aktivisten" mehr geeignet sei als für die Terrorprävention. (Lischka 2012: Link)(Wikileaks 2012: Link). Besonders brisant an Trapwire ist, dass es das System der Überwachung des öffentlichen Raumes weitgehend privatisiert. Alle durch Kameras erhobenen Informationen werden zwar in einer zentralen Datenbank gespeichert, jedoch tragen immer mehr private Firmen Informationen zu dieser Datenbank mit bei. Zum Beispiel sind viele Kasinos in Las Vegas, sowie öffentliche Institutionen Teil dieses Systems und können Daten einspeisen und darauf zugreifen, um mögliche Risiken zu erkennen. (Biermann 2012: Link). Dabei werden solche Systeme heimlich, ohne Wissen der Öffentlichkeit in immer größerem Umfang aufgebaut, ohne dass dabei eine demokratische Kontrolle stattfindet. Ohne den Anonymous Hack gegen Stratfor

wäre die Existenz von Trapwire wohl niemals der Öffentlichkeit bekannt geworden. Interessant ist, dass es sich bei Trapwire nicht um ein staatliches Überwachungsprogramm nur von CIA/NSA handelt, sondern um eine Offensive, welche maßgeblich von privatwirtschaftlich agierenden Konzernen getragen wird.

Bisher werden die Algorithmen zwar nur im Bereich der Sicherheit eingesetzt, eine Ausweitung auf andere Gesellschaftsbereiche scheint jedoch nicht unmöglich zu sein. So könnten zum Beispiel Krankenkassen ähnliche Technik einsetzen, um das Risiko zu analysieren, mit welchem ein möglicher Kunde erkrankt. Oder Universitäten könnten Algorithmen verwenden ,um anhand personenbezogener Daten die Wahrscheinlichkeit zu berechnen, mit welcher Wahrscheinlichkeit ein Student sein Studium erfolgreich benden wird. Dies könnte dann von seiten der Privatwirtschaft auch herangezogen werden, um über die Vergabe von Studienkrediten bzw die dafür fällige Verzinsung zu entscheiden. Der totalen Ökonomisierung aller Lebensbereiche wären somit quasi keine Grenzen mehr gesetzt. An den internationalen Finanzmärkten werden schon jetzt ein Großteil der Transaktionen automatisiert von Algorithmen getätigt, diese können mehr Informationen erfassen und schneller reagieren als menschliche Händler.
Auch wäre es theorethisch denkbar das am Arbeitsmarkt die Algoryithmen die Leistungsfähigkeit und Risiken von möglichen Arbeitnehmern bewerten könnten und so Empfehlungen für Einstellungen vorbereiten können.

So entsteht, ermöglicht durch den Technologischen Fortschritt, aber vor allem auch durch die zunehmende Verschmelzung von staatlicher und privatwirtschaftlicher Sicherheit, die Gefahr eines zunehmenden Algorithmen gesteuerten Totalitarismus, welcher potentiell in der Lage ist, alle Lebensbereiche zu erfassen und durch individuelle Risikoanalysen vollständig zu ökonomisieren. Zwar stehen dem zum Beispiel in Deutschland noch ein starker verfassungsrechtlich geschützer Datenschutz entgegen, in anderen Ländern wie den USA scheint dies jedoch kaum der Fall zu sein. Auch der Widerstand gegen den immer weiteren Ausbau der Sicherheit hält sich, einmal abgesehen von Occupy oder der Hackerbewegung in Grenzen, sodass einem weiteren Ausbau dieser Strukturen nicht viel im Wege steht.

Auch wenn Kannankulams These, der Neoliberalismus benötige ein stärkeres Sicherheitsregime, berechtigt ist und dies sicherlich dazu beiträgt, dass das Sicherheitssystem schneller ausgebaut wird, so ist es doch eher unwahrscheinlich, dass z.B. in der McCarthy-Ära solche Technologie, hätte sie Verfügung gestanden, nicht eingesetzt worden wäre.
Die Erweiterung der staatlichen Sicherheit erfolgte in den letzten Jahren verstärkt im Ausbau der digitalen Überwachungsinfrastrukturen und stellt somit eine Anpassung des bereits bestehenden Sicherheitsregimes an die neuen technologischem Möglichkeiten dar.
Nicht zuletzt ergibt sich hier für die Befürworter eines umfassenden Sicherheitsstaates die Chance, klassische Bürgerrechte zu umgehen. Gab es bei der Volkszählung 1987 noch massive Proteste und Wiederstände seitens der Zivilgesellschaft, so führte die Bekanntgabe, dass der BND Millionen von Emails ohne Anfangsverdacht scannt, zu keinerlei öffentlichen Empörung oder sonstigen Versuchen, diese Praxis zu unterbinden. Das Briefgeheimniss im Internet ist also de facto still und heimlich abgeschafft worden, ohne das es jemanden zu interessieren scheint. Solch weitreichende Überwachung geschieht, obwohl das Bundesverfassungsgericht die Vorratsdatenspeicherung für illegal erklärt hat. Die Strukturen des Sicherheitssystems scheinen, obwohl es sich um eine demokratische Staatsform handelt, außerhalb des Rechts zu stehen und keiner demokratischen Kontrolle mehr zu unterliegen. Hinzu kommt das zunehmende Zusammenwachsen mit Akteuren der freien Marktwirtschaft.

Ein weiterer interessanter Faktor der Globalisierung der Kommunikation ist, dass solche Überwachungsmaßnahmen auch über Ländergrenzen hinweg zunehmend einfacher werden. Sei es durch den Einsatz staatlicher bzw geheimdienstlicher Trojaner oder mittels Cloud Computing. Die

großen Konzerne, seien es Google, Microsoft oder Apple, speichern ihre Daten in Rechenzentren in den USA, auf welche die US Behörden mehr oder weniger freien Zugriff haben. Vor allem Apple und Microsoft koppeln ihre proprietären Betriebssysteme immer enger an ihre Cloud Angebote, so dass immer mehr Nutzer Backups ihrer gesamten Datenbestände auf Servern in den USA liegen haben. Diese können natürlich technisch gesehen mühelos ausgewertet und für die Erstellung von Profilen verwendet werden. Vor dieser Problematik warnen nun das Centre D'Etudes Sur Les Conflits und des Centre for European Policy Studies in einer gemeinsamen Studie (EU Parlament: Link). Aus diesen Datenbergen ließen sich durch entsprechende Algorithmen Aussagen über die weltweite gesellschaftliche und ökonomische Entwicklungen sowie Privatpersonen treffen und statistisch auswerten. Selbst die Deutsche Politik ist mittlerweile von dieser Problematik betroffen, so stellte die Landtagsfraktion der Piratenpartei in Nordrhein-Westphalen, fest, dass der Landtag eine Spamfiltersoftware von Google nutzt. Der US Konzern somit also direkten Zugriff auf den vertraulichen Emailverkehr der Abgeordneten und Mitarbeiter des Landtages habe. (Deutsche Presse Agentur 2012: Link)
Der Rücktritt von CIA Chef Petraeus zeigt, dass selbst die geheimdienstlich-staatlichen Eliten nicht vor der Speicherwut der Privatwirtschaft sicher sind. Denn Agenten des FBI überwachten Patreus privaten Email Account bei Google und erfuhren somit von der außerehelichen Beziehung des CIA Geheimdienstgenerals. (Hasselman, Silke 2012: Link)
Dass selbst die Sicherheitsfirmen und der Staat nicht die absolute Kontrolle über die angehäuften Daten ausüben, zeigen zum Beispiel die Leaks hundertausender geheimer Militärdokumente aus dem Irak und Afghanistankrieg durch Wikileaks. Am 24 Dezember 2011 gelang es der Hackergruppe Anonymous, die auch als "Schatten CIA" bezeichnete Geheimdienstfirma Stratfor zu hacken. Dabei wurden mehr als 200 Gigabyte an Daten endwendet und Teile davon später auf Filesharing Plattformen geleakt. (Volkery 2012: Link) Aus diesen Daten wird ersichtlich das Stratfor nicht nur für staatliche Stellen arbeitet, zu den Auftraggebern gehören auch Banken und private Konzerne. So lässt z.B. Coca Cola Aktivisten der Tierschutzgruppe Peta durch Stratfor überwachen.

Verschmelzung von Staatlicher und Privatwirtschaftlicher Sicherheit

Es hat also den Anschein, dass durch das Zusammenwirken von Digitalisierung und Neoliberalismus staatliche und privatwirtschaftliche Akteure in zunehmenden Maße miteinander verschmelzen. Vor allem der Staat ist in einem immer höhren Maße auf die Privatwirtschaft angewiesen, um die Sicherheit weiter ausbauen zu können. Dies liegt nicht zuletzt daran das die Privatwirtschaft mittlerweile einen entsprechenden technologischen Vorsprung hat und das "Geistige Eigentum" an Algorithmen und Technologie bei privaten Anbietern liegt. Firmen wie Raytheon besitzen also alle Rechte an der entsprechenden Analyse-Software und lizenzieren diese an den Staat. Will der Staat die entsprechenden Infrastrukturen aufrecht erhalten, ist der dazu permanent auf jene privaten Konzerne angewiesen, welche die dafür notwendige Technik, Software und Datenbestände liefern.

Diese Verschmelzung scheint jedoch nicht nur im Bereich der Sicherheit der Fall zu sein, die Einflussnahme privatwirtschaftlicher Interessen auf die Politik wird auch in anderen Bereichen immer stärker. Dies lässt sich auch bei der derzeitigen Wirtschaftskrise beobachten. Sogenannte systemrelevante Banken werden mit Unsummen an Steuergeldern gerettet, während gleichzeitig in europa ganze Volkswirtschaften in den Ruin gespart werden und das soziale Elend weiter zunimmt. Die Privatisierung der Öffentlichen Sicherheit scheint hier nur ein kleiner Teil einer viel größeren Machtverlagerung inerhalb von Politik und Ökonomie zu sein. Welche zwar innerhalb der Demokratie stattfindet diese aber zunehmend außer Kraft setzt. Da der Widerstand gegen solche Vorhaben relativ schwach ausfällt ist für die Zukunft damit zu rechnen das die Systeme der inneren Sicherheit weiter ausgebaut werden und privatwirtschaftliche Interessen weiter an Macht gewinnen.

Quellen:

Kannankulam, John (2009): Zur politischen Ökonomie der inneren Sicherheit und ihres Wandels
In: rechtprogressiv
http://www.rechtprogressiv.de/wp-content/uploads/2009/05/Kannankulam_Innere-Sicherheit-2009.pdf (10.01.2013)

Dozier, Kimberly, (2011): Wie die CIA soziale Netze überwacht
In: sueddeutsche
http://www.sueddeutsche.de/digital/geheimdienst-bei-facebook-und-co-wie-die-cia-soziale-netze-ueberwacht-1.1183886 (12.01.2013)

Simonite, Tom (2010): Digitale Kristallkugel
In: Heise
http://www.heise.de/tr/artikel/Digitale-Kristallkugel-1147791.html (12.01.2013)

Der Spiegel (2012): Regierung hält Details der Internet-Überwachung geheim
In: Spiegel http://www.spiegel.de/netzwelt/netzpolitik/regierung-haelt-details-der-e-mail-ueberwachung-geheim-a-834897.html (11.01.2013)

Talbot, David (2012): Der maschinelle Analyst
In: Heise
http://www.heise.de/tr/artikel/Der-maschinelle-Analyst-1627174.html (10.01.2013)

Beuth, Patrick (2011): Die Polizei als Hellseher
In: Zeit
http://www.zeit.de/digital/datenschutz/2011-08/predictive-policing (11.01.2013)

Bland, Eric (2010): Software Predicts Criminal Behavior
In: ABC News
http://abcnews.go.com/Technology/software-predicts-criminal-behavior/story?id=11448231#.UOxeUxWrr4t (13.01.2013)

Lischka, Konrad (2012): Software vernetzt Videoüberwachung
In: Spiegel
http://www.spiegel.de/netzwelt/netzpolitik/trapwire-wikileaks-veroeffentlicht-details-zu-ueberwachungssoftware-a-849761.html (12.01.2013)

Wikileaks (2012): The Global Intelligence Files
In: Wikileaks
http://wikileaks.org/gifiles/releasedate/2012-08-12-08-trapwire-multi-country-surveillance-network.html (13.01.2013)

Biermann, Kai (2012): Trapwire spioniert Bürger in großem Stil aus – Privatisierte Überwachung aller Bürger. In: Zeit
http://www.zeit.de/digital/datenschutz/2012-08/trapwire-wikileaks/seite-3 (12.01.2013)

Centre D'Etudes Sur Les Conflits / Centre for European Policy Studies (2012):
In: Europarl
http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050 (11.01.2013)

Deutsche Presse Agentur (2012): Wenn Google im Landtag mitliest
In: Taz
http://www.taz.de/!103617/ (11.01.2013)

Hasselmann, Silke (2012): Trat Petraues wegen FBI Ermittlungen zurück ?
In: Tagesschau
http://www.tagesschau.de/ausland/petraeus-cia104.html (12.01.2013)

Volkery, Carsten (2012): Wikileaks blamiert die “Schatten-CIA”
In: Spiegel
http://www.spiegel.de/netzwelt/netzpolitik/stratfor-hack-wikileaks-blamiert-die-schatten-cia-a-817838.html (13.01.2013)

